

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Digital Output Protection Technology and Recording Method Certifications)	MB Docket No. 04-66
)	
Windows Media Digital Rights Management Technology)	

**OPPOSITION TO THE APPLICATION OF MICROSOFT FOR INTERIM
AUTHORIZATION OF WINDOWS MEDIA DRM BY THE MOTION PICTURE
ASSOCIATION OF AMERICA, INC., METRO-GOLDWYN-MAYER STUDIOS INC.,
PARAMOUNT PICTURES CORPORATION, SONY PICTURES ENTERTAINMENT
INC., TWENTIETH CENTURY FOX FILM CORPORATION, UNIVERSAL CITY
STUDIOS LLLP, THE WALT DISNEY COMPANY, AND WARNER BROS.
ENTERTAINMENT INC.**

Jon A. Baumgarten
Bruce E. Boyden
Proskauer Rose LLP
1233 Twentieth Street NW, Suite 800
Washington, DC 20036
(202) 416-6800

April 6, 2004

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	1
I. WMDRM Does Not Place Meaningful Restrictions on the Scope of Redistribution of Marked and Unscreened Content	3
II. Microsoft Has Provided Inadequate Information as to the Security of WMDRM	6
III. WMDRM Does Not Contain Adequate Compliance or Robustness Rules	6
IV. Microsoft's Application Does Not Provide for Effective Revocation and Renewability	9
V. WMDRM Does Not Provide for Adequate Enforcement	10
VI. WMDRM Does Not Provide for Fair Change Management	11
VII. No Compelling Justification Has Been Offered in Support of Authorization of WMDRM	11
A. The Need for Open Platform Technologies Does Not Justify Interim Authorization of WMDRM	11
B. There Has Been No Content Owner Use or Approval of WMDRM for Broadcast Content	12
VIII. If Microsoft Resubmits Its WMDRM Application, It Should Facilitate Ready Discussion by Clarifying That It Is Bound to WMDRM's License and That WMDRM Imposes No Obligations on Content Providers, Broadcasters, and Others	13
CONCLUSION	15

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)	
)	
Digital Output Protection Technology and Recording Method Certifications)	MB Docket No. 04-66
)	
Windows Media Digital Rights Management Technology)	

**OPPOSITION TO THE APPLICATION OF MICROSOFT FOR INTERIM
AUTHORIZATION OF WINDOWS MEDIA DRM BY THE MOTION PICTURE
ASSOCIATION OF AMERICA, INC., METRO-GOLDWYN-MAYER STUDIOS INC.,
PARAMOUNT PICTURES CORPORATION, SONY PICTURES ENTERTAINMENT
INC., TWENTIETH CENTURY FOX FILM CORPORATION, UNIVERSAL CITY
STUDIOS LLLP, THE WALT DISNEY COMPANY, AND WARNER BROS.
ENTERTAINMENT INC.**

The Motion Picture Association of America, Inc. (“MPAA”), Metro-Goldwyn-Mayer Studios Inc., Paramount Pictures Corporation, Sony Pictures Entertainment Inc., Twentieth Century Fox Film Corporation, Universal City Studios LLLP, The Walt Disney Company, and Warner Bros. Entertainment Inc. (collectively, “the MPAA Parties”) hereby submit this opposition to the application of Microsoft for interim authorization for Windows Media Digital Right Management Technology (“WMDRM”).¹

INTRODUCTION

Microsoft’s WMDRM holds the promise of making secure digital broadcast television available to every modern Windows PC. Unfortunately, the technology as proposed in the

¹ See Certification of Windows Media Digital Rights Management Technology for Use With Broadcast Flag, M.B. Docket No. 04-66 (filed Mar. 1, 2004).

Application submitted by Microsoft does not achieve the goals of the Broadcast Flag Report & Order and is not ready to be authorized for use with Marked and Unscreened Content at this time because, among other reasons, it does not place meaningful restrictions on the scope of redistribution of Marked and Unscreened Content. The MPAA Parties look forward to working with Microsoft to improve its technology for ultimate approval by the Commission. The critical issues that would need to be addressed by such a future filing are: (1) the development of effective restrictions on the scope of redistribution of broadcast content; (2) information concerning the security of WMDRM; (3) the addition of compliance and robustness rules; and (4) the failure to provide for a meaningful content provider role in revocation, renewal, enforcement, and change management. In addition, to facilitate ready consideration of any future filing, Microsoft should also confirm that Microsoft will itself be bound by the terms of the WMDRM license, and that WMDRM places no obligations on content providers, broadcasters, and others.

We note at the outset that this proceeding, and the Commission's review of the content protection technologies, related functionalities, and licenses submitted in this proceeding, are concerned only with whether the proposal meets the interim requirements the Commission identified for the protection of digital broadcast television content. This response, therefore, is based on the understanding that if the Commission decides to authorize WMDRM on an interim basis for use in protecting Marked and Unscreened Content, which the MPAA opposes for the reasons set forth herein, that authorization extends only to the use of WMDRM in the Broadcast Flag application.²

² For example, the interim authorization of a content protection technology would not determine in any way whether that technology appropriately protects content with copy restrictions delivered through high-definition analog outputs, which was not the subject of the Broadcast Flag proceeding.

I. WMDRM Does Not Place Meaningful Restrictions on the Scope of Redistribution of Marked and Unscreened Content

WMDRM does not provide any meaningful restriction on the scope of redistribution of Marked and Unscreened Content, either in downstream devices by means of compliance rules or in the Covered Demodulator Product itself. Although the descriptive material explicitly refers to enabling distribution “within the home,” no mechanism limiting such distribution is identified. WMDRM is not currently using any proximity controls to manage the distribution of the keys for decrypting the Broadcast Flag content only to “authenticated” WMDRM devices located within the same local home network. The descriptive material indicates that “proximity” elements may be added in the future and doing so will go a long way to meeting the objectives of the Broadcast Flag proceeding and achieving eventual authorization of WMDRM.

Under Microsoft’s Application, each Windows PC running WMDRM applications could distribute through streaming Marked and Unscreened Content to every other Windows PC or networked streaming device using WMDRM. Additionally, although unclear, it appears from the Microsoft Application that such distributions can be made to any “authorized connected media storage devices implementing WMDRM.” While those transmissions would be encrypted, every PC using WMDRM wherever located could have the ability to decrypt the content.

The addition of device limits alone, without proximity controls, would not measurably improve the Microsoft Application for the current version of the technology. Such a system would still allow unauthorized redistribution to at least a few devices outside the local broadcast market per receiver. While redistribution to two or three persons out-of-market may not hurt local broadcasting, that effect would be multiplied by the number persons receiving the initial broadcast. In addition, unconstrained redistribution to two or three persons per initial recipient

would have a cascade effect, given that the program could then be further redistributed to two or three more persons, *ad infinitum*. The number of simultaneous connections permitted is therefore irrelevant; what is relevant is how far and how easily the content may be transmitted from the Covered Demodulator Product.

Microsoft may also in the future propose adding personal affinity-based mechanisms to WMDRM to control redistribution. However, in the context of this interim process, technologies that rely on personal affinity-based mechanisms alone raise too many difficult technological, policy, privacy, and legal questions that are not appropriately addressed in this proceeding. The use of personal affinity-based controls, without proximity controls, would essentially allow consumers to be retransmitters of content owned by others, a far-reaching situation never before faced by the Commission, and new as well to content providers, broadcasters, manufacturers, and others, including even consumers themselves. Physical redistribution, which has been in existence for years, is well understood; however, there are difficult questions concerning what technological limits need to be placed on consumer retransmission such that content owners' rights are not trampled and the digital transition thwarted. These are not the sort of issues that are appropriately addressed in an accelerated, interim proceeding.

In exchanges during the proceeding which led to this interim certification procedure, reference was occasionally made to the notion of "remote access" – that is, to circumstances under which the technology need not inhibit, and indeed might facilitate, transmission to locations remote from the home receiver. The MPAA Parties are not opposed to that notion as such; however, we strongly believe that careful consideration of numerous interrelated practical, business, legal, and technological considerations which underlie the appropriate "circumstances" is a fundamental necessity and complex undertaking – including a threshold issue of whether it is

better suited to government involvement or marketplace resolution.³ Converting the consumer to a re-broadcaster is a far-reaching step; for that reason we believe it is premature, inappropriate, and counterproductive to approve in this interim proceeding this or any other technology which, on the present record at least and unless modified or sufficiently clarified, does not take meaningful and affirmative steps to limit redistribution by proximity to the home receiver.

Technologies considered for interim authorization must therefore contain, as a necessary condition, proximity controls that approximate the physical constraints that have heretofore prevented consumers from being retransmitters. Limiting the “proximity” means that the technology affirmatively and reasonably constrains unauthorized redistribution from extending beyond a Covered Demodulator Product’s local environment – i.e., the set of compliant, authorized devices within a tightly defined physical space around that product. Affirmative and reasonable constraints may include the use of controls to limit distance from a Covered

³ The remote access issue is precisely presented under the heading of “personal digital network environment” (to the extent it extends beyond the home, the PDNE is essentially a remote-access zone) in the Commission’s Further Notice of Proposed Rulemaking in the Docket No. 02-230, FCC 03-273 (rel. Nov. 4, 2003). *The conclusion of that inquiry should not be predetermined in this relatively summary and fast track proceeding. Moreover, comments in that docket generally agreed that it was premature, at best, to address this issue. See, e.g.,* Comments of MPAA *et al.* at 8 (“[A]n attempt to regulate or define this area will inevitably risk substantial and continuing conflict with copyright law definitions of exclusive rights pertaining to performance and distribution, and significantly impair if not render impossible the efforts of copyright owners to protect those right by technological means. *It will also fundamentally impair and interfere with emerging business models designed to enhance consumer choice and consumer enjoyment of remote usage technologies.*”) (emphasis added); Comments of Time Warner Inc. at 10-12 (noting and illustrating, *inter alia*, “substantial effect and alter[ation] of existing video distribution agreements and business models”; “implica[tion] of significant and controversial copyright law issues”; provoking “protracted legal conflicts and consumer confusion”; existing cross-industry efforts to “accommodate consumer interests to use content flexibly”; enmeshing and undermining pre-existing business and licensing relationships including geographic limitations that “are particularly important in the broadcast television context, since many broadcast programs are licensed to television stations pursuant to strict and well-defined local market restrictions”); Comments of the Office of the Commissioner of Baseball *et al.* at 6-7 (concern that remote access regimes “must be consistent with copyright owners rights” and “go no further than copyright law permits”). Although differing with the MPAA parties on rationale (and hence reinforcing the Time Warner prediction of “protracted legal conflict”) the Comments of Public Knowledge and Consumers Union (at 11-12) explicitly acknowledged that defining a PDNE “will tread on the prerogatives of Congress in defining copyright law and associated doctrines such as fair use.” Other commenting parties rejected the need for a government defined PDNE or zone of remote access on grounds that differ from the MPAA parties but, like those of Public Knowledge and Consumers Union, amply forecast the contentious and difficult nature of the exercise, which far transcends the limited scope and purpose of the instant proceeding. *See, e.g.,* Comments of the IT Coalition at 6-8; Comments of Digital Transmission Licensing Administrator LLC at 16-17.

Demodulator Product, or limits on the scope of the network addressable by such Covered Demodulator Products. Personal affinity-based controls that approximate association of such set of devices with an individual or household may be beneficial to use in addition to such proximity constraints, but are not a substitute for them at this time.

In any event, Microsoft has not at this time proposed personal affinity-based mechanisms or numeric device limits for use with WMDRM. If Microsoft re-submits its Application, the MPAA Parties believe that effective proximity controls should be added. The MPAA Parties look forward to working with Microsoft to improve its submission in this regard.

II. Microsoft Has Provided Inadequate Information as to the Security of WMDRM

Microsoft did not state how WMDRM will protect Marked and Unscreened Content. For instance, Microsoft's certification mentions that a certain list of technologies is included in WMDRM, but it does not detail the cryptographic strength or level of security provided by those technologies. There is thus insufficient information for the Commission and others to evaluate the level of security for digital broadcast content provided by WMDRM.

III. WMDRM Does Not Contain Adequate Compliance or Robustness Rules

A secure content protection technology is entirely ineffective if its license does not impose restrictions on adopting downstream devices to require equivalent protection of the content downstream. This is usually achieved by the use of compliance and robustness rules. By "compliance and robustness rules" we mean provisions in license agreements for use of the technology that (a) require a Covered Demodulator Product and downstream licensees to properly implement encryption, decryption, authentication, revocation and renewal (as appropriate), and limitations on the scope of redistribution; (b) perpetuate the digital output and digital recording rules of the Broadcast Flag Regulation serially downstream from Covered

Demodulator Products; and (c) require robust implementations. It is critical that these downstream obligations be adequately and clearly imposed by license, since after broadcast content leaves a Covered Demodulator Product via an authorized output, that content and the devices receiving it are generally removed from the ambit of the Broadcast Flag regulation. Thus, the redistribution control that the FCC has concluded is critical to the digital transition must be achieved via the conditions and protections required by license on the downstream products.

There are several weaknesses with the compliance and robustness rules – of all three types listed above – proposed by Microsoft for WMDRM. First, there do not appear to be any clearly expressed compliance rules. While the license agreements submitted with the certification provide hints as to where such obligations might later be placed in revised versions of the licenses, the licenses submitted with the certification do not appear to have yet been adapted for use in connection with the Broadcast Flag.⁴

Second, the robustness rules for WMDRM are inadequate. The only robustness requirement in the Microsoft Application is contained in the Amendment to the Microsoft OEM Customer License Agreement for Embedded Systems at page 3, which provides that the “Company shall use commercially reasonable efforts to design Embedded Systems to prevent end users from tampering with the Licensed Product or the Embedded System.”⁵ Microsoft’s rule would require efforts to protect rather than protection. Furthermore, since definitions of the

⁴ For example, it appears that relevant provisions may someday be placed in the document entitled “Exhibit A: DRM License Format Requirements,” which is an exhibit to the “DRM Client Certificate Addendum to EULA for Microsoft Windows Media Format Software Development Kit 9 Series.”

⁵ This is far weaker than even the robustness standard adopted by the Commission for Covered Demodulator Products, to which the MPAA has objected, *see* Petition for Reconsideration and Clarification of the MPAA, MB Docket No. 02-230, at 2-21 (filed Jan. 2, 2004).

defined terms were not included, it is impossible to determine the level of effectiveness of this modest provision.

Even if adequate compliance and robustness rules are added, Microsoft's Application gives no indication as to how WMDRM will pass on those compliance and robustness rules to devices downstream from the Covered Demodulator Product or the initial application. This is particularly unclear with respect to the compliance rules that will perpetuate the Broadcast Flag output and recording rules (contained in Sections 73.9003 and 73.9004 of the Commission's rules). Unlike other content protection technologies being proposed to the Commission, WMDRM is not licensed by Microsoft to manufacturers to install as components at the point of output or recording in Covered Demodulator Products or downstream devices. Instead, Microsoft licenses WMDRM to software developers to integrate into applications, and to distribute those applications to end users and OEMs. But when a PC distributor installs a WMDRM application onto a preexisting PC prior to sale, or when a consumer loads a downloaded or packaged WMDRM application onto his or her existing PC, how will the WMDRM application control the operation of other recording and output functionalities in the PC so that those other functionalities comply with the compliance rules imposed on the WMDRM application developer?

Because the current Application does not address these questions, the Commission can not determine whether devices downstream from WMDRM will protect the content or instead will be free to flow out any output or be recorded in the clear, thereby frustrating the Broadcast Flag scheme.

IV. Microsoft's Application Does Not Provide for Effective Revocation and Renewability

Secure device revocation is a necessary component of any content protection technology. Similarly, a technology that is proposed for interim authorization also needs to have “renewability,” meaning the ability to be upgraded to repair or compensate for security flaws. Although Microsoft describes mechanisms for achieving WMDRM renewability, WMDRM revocation, and WMDRM-supported application revocation, all of these mechanisms assume that WMDRM devices: (i) have an online network connection for receiving revocation and renewability messages and software updates; and (ii) are being used to access other forms of WMDRM-protected, server-delivered content (e.g., Movielink content), which can deliver the renewal and revocation triggering commands that would eventually block WMDRM usage with Broadcast Flag content until renewal or revocation is executed. These assumptions may not be valid for all devices. Nor is it clear how Microsoft plans to trigger WMDRM revocation and renewal in hardware implementations of WMDRM (e.g., in a WMDRM-equipped DVD player).

The Microsoft Application also did not provide a meaningful role for content owner or broadcaster initiation and pursuit of revocation or renewal, nor does Microsoft provide any commitment to effectuate either in any case.⁶ Microsoft's Application provides for device revocation, but does not provide content owners any role in requesting that a particular device should be revoked. Instead, the revocation decision is left completely to Microsoft and the application developer. This is inadequate, however, since Microsoft will have little practical incentive to identify, investigate, and take action against compromised device keys or identity certificates. Indeed, since application developers will comprise Microsoft's primary customer

⁶ Although Paragraph 3(c) of the DRM Client Certificate Addendum to EULA for Microsoft Windows Media Format Software Development Kit 9 Series does refer to content owners “requesting” revocation, that may refer to

base, it will have every incentive not to antagonize developers by invoking revocation. It is therefore critical that content owners be provided with the right under the WMDRM license to request that device revocation be invoked, and that procedures be set forth in the license for a fair and impartial determination of the response to such a request.

Additionally, in order to effectuate revocation, renewal, or other aspects of a proposed technology that require information to accomplish a process or continued robustness or efficiency of the technology over time, it is necessary that a standardized means for delivering this information in the ATSC transport stream is developed and that FCC approval of any protected digital output and secure recording technology include obligations that Covered Demodulator Products and downstream devices properly receive, preserve, process, and convey downstream, as appropriate, such information. In any subsequent filing, Microsoft should explain how it will deal with this issue.

V. WMDRM Does Not Provide for Adequate Enforcement

Another critical component of any content protection technology is the ability of content owners to enforce the robustness and compliance requirements against manufacturers. In private agreements, this allows content owners, who have more of an interest in enforcement of the compliance and robustness rules than technology vendors, to enforce those provisions without relying on the technology manufacturer to do so. That reasoning is no less applicable in the Broadcast Flag context. The success of the Broadcast Flag regulation depends not only on the regulation itself, but also on the license terms that replicate the regulation's compliance and robustness requirements downstream. The Commission has no direct enforcement power over

other arrangements, such as under the Secure Digital Music Initiative. The procedure for such requests is nowhere reflected in the descriptive material, and no other information about it is provided.

downstream devices, and there may be no provision or resources to pursue technology licensors for failure to enforce their licenses. It is thus equally important in this context, therefore, that content providers have third-party beneficiary rights allowing pursuit of device manufacturers that breach the terms of the content protection technology license.

VI. WMDRM Does Not Provide for Fair Change Management

The WMDRM certification documents do not provide any meaningful role for content owners or broadcasters to review and participate in the approval of changes to any compliance rules, license agreements, approved downstream technologies, or technical aspects of the proposal that may be made in the future. This is an important omission, for if nothing prevents a technology manufacturer from changing the technology in material and unforeseen ways, the entire Broadcast Flag system that the Commission has worked so hard to create may come undone. Owing to the critical nature of these matters, the omission of a meaningful role for content owners or broadcasters in the Change Management process should preclude approval of WMDRM in its current form.

VII. No Compelling Justification Has Been Offered in Support of Authorization of WMDRM

A. The Need for Open Platform Technologies Does Not Justify Interim Authorization of WMDRM

Microsoft argues that its certification must be approved in order to facilitate “open platform” device participation in the Digital Transition and service of the disabled. But the mere fact that WMDRM operates on an open platform does not *ipso facto* mean that it should be approved. We would not object to an “open platform” technology that provided adequate protection against unauthorized redistribution of digital broadcasts, but Microsoft has made no showing that its technology is capable of doing so. In any event, for all the reasons the

Commission recognized in its Report and Order, adequate control over such distribution is essential to the vitality of the DTV transition. As the CE Industry has observed, if “open platform” devices can participate in DTV reception and redistribution without adequate protection of the content, then other, more secure devices will be placed at a severe competitive disadvantage.⁷

B. There Has Been No Content Owner Use or Approval of WMDRM for Broadcast Content

Although Microsoft has asserted that approval of WMDRM by content owners to entities involved in Internet delivery services is pertinent to this proceeding, Internet delivery is a very different environment. First, with respect to commercial delivery services, such as MovieLink, content providers have entered into license agreements requiring the use of specified protection technologies for secure delivery of their content with legally binding compliance and robustness rules. No such contractual relationship exists between the content provider and the technology provider when free over-the-air television containing a broadcast flag is delivered to a consumer device. The Commission’s decision with respect to WMDRM should not be influenced by prior approval of a different implementation of the technology in the context of a negotiated private license.

Second, the implementation of WMDRM in Movielink is not comparable to WMDRM as proposed for broadcast television. In the case of Movielink, content owners rely on Movielink’s secure application software to manage the distribution of encrypted content and the distribution of the WMDRM license keys for decrypting downloaded Movielink content, which can only be played one time on a single registered PC by paying customers. In the case of Broadcast

⁷ See CE Industry Opposition to Petitions for Reconsideration, MB Docket No. 02-230, at 2 (filed Mar. 10, 2004).

Flag content, however, the license key is generated locally in software, and the content is encrypted locally by the consumer's PC. The content can then be distributed over the Internet to an undefined number of WMDRM-equipped PCs for unlimited playback. As such, the risk of attack and the scope of redistribution are much greater in the latter case.

VIII. If Microsoft Resubmits Its WMDRM Application, It Should Facilitate Ready Discussion by Clarifying That It Is Bound to WMDRM's License and That WMDRM Imposes No Obligations on Content Providers, Broadcasters, and Others

The MPAA Parties request that Microsoft, as part of any resubmission of WMDRM, also respond to and/or clarify the following issues in a satisfactory manner in order to facilitate ready consideration of WMDRM technology by the Commission in this proceeding.

First, Microsoft should clarify that, when WMDRM has compliance and robustness rules, it will abide by them when it incorporates WMDRM into its own products. The critical issue is that no manufacturer of a downstream device receiving Marked or Unscreened Content should be able to do so without agreeing to follow compliance and robustness rules equivalent to those in the Broadcast Flag regulation. Microsoft should therefore clarify that for any use of the WMDRM technology, Microsoft itself is obligated to comply with the compliance and robustness rules of the WMDRM license agreement (when they are added) in the same manner as any other Adopter licensee of the WMDRM technology.

Second, Microsoft should clarify that there are no obligations that would impact content owners, broadcasters, consumers, or others described below by use of its technology. WMDRM could become one of many technologies included in the Broadcast Flag system. All approved technologies will receive broadcast content marked with the Broadcast Flag and may be invoked or "triggered" in response to the Broadcast Flag in various devices, such as set-top boxes and digital video recorders. Content providers, broadcasters, and others currently cannot direct

which approved technologies may receive broadcast content marked with the Broadcast Flag or which approved technologies may get triggered by the Broadcast Flag. Because content providers, broadcasters, and others exercise no direct control over the actual use of WMDRM (or any of the other potential approved technologies), Microsoft should clarify that broadcasters, content providers, and others who do not take a license to the WMDRM technology but who mark or broadcast content with a Broadcast Flag that triggers WMDRM are not subject to any obligations to Microsoft, including but not limited to intellectual property licensing obligations. Furthermore, Microsoft should certify, as a condition of interim authorization, that no consumer transmitting or receiving content marked with the Broadcast Flag signal will incur any claim of obligation from Microsoft.

* * *

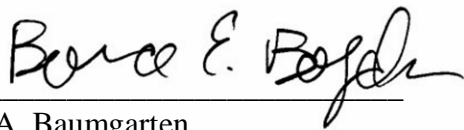
CONCLUSION

Although the MPAA Parties look forward to working with Microsoft further in developing its Windows Media DRM technology for ultimate Commission authorization, at this time, for the reasons stated above, the application of Microsoft for interim authorization of Windows Media DRM should be rejected.

Respectfully submitted,

THE MOTION PICTURE ASSOCIATION OF AMERICA, INC.
METRO-GOLDWYN-MAYER STUDIOS INC.
PARAMOUNT PICTURES CORPORATION
SONY PICTURES ENTERTAINMENT INC.
TWENTIETH CENTURY FOX FILM CORPORATION
UNIVERSAL CITY STUDIOS LLLP
THE WALT DISNEY COMPANY
WARNER BROS. ENTERTAINMENT INC.

By: _____



Jon A. Baumgarten

Bruce E. Boyden

Proskauer Rose LLP

1233 Twentieth Street NW, Suite 800

Washington, DC 20036

(202) 416-6800

Counsel for the Commenting Parties